PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/16, H04Q 7/38 — A1

(11) International Publication Number: WO 97/12461

(43) International Publication Date: 3 April 1997 (03.04.97)

(21) International Application Number: PCT/SE96/01156

(22) International Filing Date: 18 September 1996 (18.09.96)

(30) Priority Data:
9503343-7 27 September 1995 (27.09.95) SE

(71) Applicant *(for all designated States except US)*: TELEFONAKTIEBOLAGET LM ERICSSON (publ) [SE/SE]; S-126 25 Stockholm (SE).

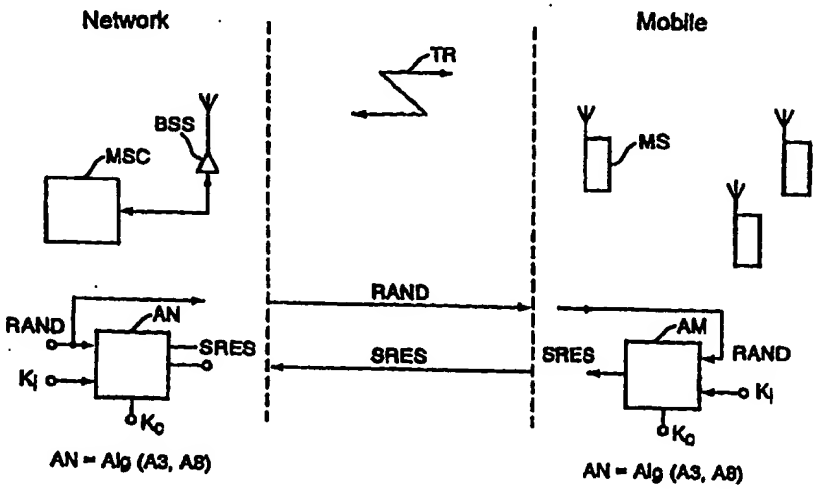
(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: BODIN, Roland [SE/SE]; Gribbyvägen 55, S-163 59 Spånga (SE).

(74) Agents: BOHLIN, Björn et al.; Telefonaktiebolaget LM Ericsson, Patent and Trademark Dept., S-126 25 Stockholm (SE).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
With amended claims.
In English translation (filed in Swedish).

(54) Title: METHOD FOR ENCRYPTION OF INFORMATION



(57) Abstract

The present invention relates to various methods of encrypting an information flow (speech or data) which is to be transmitted in a mobile radio system. The mobile radio system transfers information in accordance with the time division multiple access concept (TDMA) between a network (MSC, BSS) and a specific mobile station (MS) from among a plurality of mobile stations. The proposed encryption methods are used when information (B1, B2) of a given user shall be transferred in two or more time slots (TS1, TS2) within a single frame. In accordance with the inventive encryption methods, the various parameters (Kc, FN, PS) used in the encryption process are modified in dependence on the ordinal number of each of the used time slots in a frame. For instance, the encryption key (Kc) and the frame number (FN) are modified in dependence on the ordinal number (TSn) of the relevant time slot and the known encryption algorithm (A5) is used to obtain a modified encryption sequence (PSm'). This obviates the need to make substantial changes to the system signalling protocols and hardware.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	GB	United Kingdom	MW	Malawi
AT	Austria	GE	Georgia	MX	Mexico
AU	Australia	GN	Guinea	NE	Niger
BB	Barbados	GR	Greece	NL	Netherlands
BE	Belgium	HU	Hungary	NO	Norway
BF	Burkina Faso	IE	Ireland	NZ	New Zealand
BG	Bulgaria	IT	Italy	PL	Poland
BJ	Benin	JP	Japan	PT	Portugal
BR	Brazil	KE	Kenya	RO	Romania
BY	Belarus	KG	Kyrgystan	RU	Russian Federation
CA	Canada	KP	Democratic People's Republic of Korea	SD	Sudan
CF	Central African Republic			SE	Sweden
CG	Congo	KR	Republic of Korea	SG	Singapore
CH	Switzerland	KZ	Kazakhstan	SI	Slovenia
CI	Côte d'Ivoire	LI	Liechtenstein	SK	Slovakia
CM	Cameroon	LK	Sri Lanka	SN	Senegal
CN	China	LR	Liberia	SZ	Swaziland
CS	Czechoslovakia	LT	Lithuania	TD	Chad
CZ	Czech Republic	LU	Luxembourg	TG	Togo
DE	Germany	LV	Latvia	TJ	Tajikistan
DK	Denmark	MC	Monaco	TT	Trinidad and Tobago
EE	Estonia	MD	Republic of Moldova	UA	Ukraine
ES	Spain	MG	Madagascar	UG	Uganda
FI	Finland	ML	Mali	US	United States of America
FR	France	MN	Mongolia	UZ	Uzbekistan
GA	Gabon	MR	Mauritania	VN	Viet Nam

This Page Blank (uspto)

METHOD FOR ENCRYPTION OF INFORMATION

FIELD OF INVENTION

The present invention relates to a method of encrypting information between a stationary network and a mobile station in a mobile radio system of the time division multiple access type (TDMA system).

More specifically, the invention relates to methods of encrypting the transmitted information in a more secure fashion in conjunction with an authorization check on the mobile by the network and when a multiple of time slots are used for the same user (mobile station).

DESCRIPTION OF THE BACKGROUND ART

The GSM-network, common in Europe, is a mobile radio network that uses time division multiple access (TDMA). As with other mobile radio networks, the GSM network employs authorization checks and encryption of transmitted messages. With regard to the GSM network, this is specified in "GSM specification 03.20", May 1994, issued by ETSI (European Telecommunication Standard Institute) and hereinafter referred to as ETSI/GSM 03.20. The various algorithms used in authorization checks and encryption are described in this reference.

An algorithm A3 is used to effect actual authorization checks between network and subscriber apparatus, an algorithm A5 is used for encryption of the payload information to be transmitted, and an algorithm A8 is used to form from the subscriber authorization key Ki an encryption key Kc from a random number variable, RAND.

As a rule, only one time slot per frame for a given connection is used in TDMA-type time division mobile radio systems; see ETSI/GSM 05.02.

The use of two or more time slots, not necessarily consecutive time slots, in a transmission frame has been proposed, see ETSI/STC SMG3, T doc SMG3 WPA 95A dated 29th August 1995 (Nokia Telecommunications), see particularly point 5 "HSCSD Architecture". This provides the advantage of enabling larger quantities of information to be transmitted per unit of time (applicable particularly to data transmissions), but has the drawback of increasing bandwidth.

SUMMARY OF THE INVENTION

The inclusion in a GSM system of two or more time slots instead of one time slot for one and the same radio transmission in accordance with the aforegoing creates certain problems when encryption and authorization checks are to be employed.

The most obvious procedure would be to process each of the time slots separately and to process the information in accordance with earlier known principles. However, such procedures would require drastic modification to the existing signalling protocols and to equipment on both the network side and the mobile station side.

It would be desirable to avoid such modifications to existing standards and equipment to the greatest possible extent. The use of the same pseudo-random sequence for all time slots within one and the same frame and for a given frame number is proposed in the aforementioned ETSI document, ETSI/ T doc SMG3, "First HSCSD stage 2 draft". The drawback with this method is that it is necessary to compromise between encryption safety and procedure simplicity. When two separate bursts belonging to one and the same user are transmitted in this manner while using the same encryption sequence (pseudo-random random sequence), the influence of the encryption can be eliminated relatively simply, by carrying out simple EXOR operations.

The object of the present invention is therefore to provide methods for reliable encryption in respect of authorization checks in a TDMA-type mobile radio system in which two or more time slots are used for one and the same transmission without needing to make substantial changes to the signalling protocol and/or system equipment.

In this regard, an inventive method is characterized by the features set forth in the following Claim 1. Another inventive method is characterized by the features set forth in the accompanying Claim 3. Further inventive methods are characterized by the features set forth in accompanying Claims 4 and 5.

BRIEF DESCRIPTION OF THE DRAWINGS

The aforesaid inventive methods will now be described in more detail with reference to the accompanying drawings.

Figure 1 illustrates schematically signalling between a network side and a mobile station side in a mobile radio system during the authorization check procedure.

Figure 2 is a block diagram illustrating known information encryption in the system illustrated in Figure 1.

Figure 3 is a block diagram which symbolizes the algorithms used in two of the inventive methods.

Figure 4 is a block diagram symbolizing the algorithms used in a third inventive method.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Figure 1 is a simplified schematic illustration of a mobile radio system, for instance a GSM-system. The system has a network side "NETWORK" and a mobile station side "Mobile".

The network side includes a base station system BSS which is connected to a mobile switching centre MSC, which is connected, in turn, to the public telephone network (not shown). The base station system BSS typically includes a base transceiver station BTS and a base station controller BSC (not shown). In reality, a plurality of base station systems are connected to the mobile switching centre MSC on the network side, while the mobile station side includes a plurality of mobile stations that can communicate simultaneously with the base station system BSS. The network side and the mobile station side transmit information via radio signals over an air interface which is symbolized in Figure 1 with the reference TR.

Before the actual information is transmitted and received between the network and a given mobile station MS, the network is obliged to check the authorization of the mobile station MS. This authorization check is carried out in accordance with known principles, whereby the network, i.e. the base station system BSS, sends a random number (so-called "random challenge") RAND to the mobile station MS over a dedicated control channel DCCH.

The mobile station MS receives the random number RAND and forms a response SRES (signed response) from this random number and from the mobile station's own key Ki in accordance with a given algorithm A3, as described on page 50 of the aforesaid ETSI/GSM 03.20.

At the same time, the mobile station MS compiles an encryption key Kc from the key Ki in accordance with another algorithm A8, although only the response SRES is sent to the base station system BSS, while the encryption key Kc is used in the encryption carried out in the mobile station in accordance with the following. A comparison is made in the base station system BSS with corresponding values of SRES calculated by the mobile switching center (MSC) in accordance

with the same conventional algorithms A3 and A8 found in the mobile station MS. When a coincidental result is obtained, the mobile station is considered to be authorized and communication can continue. The continued information transmission will thereafter be encrypted in accordance with a given algorithm A5, as described on pages 48-49 of ETSI/GSM 03.20.

Thus, the network includes an algorithm block AN which stores and carries out an authorization check in accordance with the algorithms A3 and A8 and encryption in accordance with the algorithm A5. The mobile station MS includes a corresponding algorithm block AM which stores and carries out an authorization check in accordance with the same algorithms A3 and A8 and encryption in accordance with the algorithm A5.

The encryption key Kc is generated by the mobile switching center (MSC) on the basis of the mobile station's encryption key Ki, which is known to the mobile telephone switching centre. Subsequent to making the authorization check, (algorithm A5), the mobile telephone switching centre MSC sends the key Kc to the base station system BSS and encryption of payload information can be commenced with the aid of the agreed encryption key Kc.

Figure 2 illustrates schematically the manner in which the payload information is encrypted and formatted for transmission over two time slots TS1, TS2 in accordance with the aforesaid NOKIA proposal.

Normally, the payload information is divided from, e.g., a speech frame into one or more blocks each of 114 bits. One such block is encrypted in accordance with the algorithm A5 and sent during a burst in a given time slot, optionally interfoliated with another adjacent block. The next encrypted block then follows. As illustrated in Figure 2, when two time slots in a given frame are available, an information block

is now divided into two sub-blocks B1 and B2, each containing 114 bits, and each block is encrypted with the same pseudo-random sequence PS of 114 bits as normal, by carrying out two EXOR operations shown in Figure 2.

The pseudo-random sequence PS is obtained from an ordinal number FN of the frame in which the time slots TS1, TS2 are located whose information (blocks B1 and B2) shall be encrypted. Two encrypted information blocks BK1 and BK2 are obtained and these blocks are then formatted by inserting a sync. and training sequence in a known manner (marked with X in Figure 2). As before mentioned, the drawback with this encryption method is that the same encryption sequence is used two times for two separate time slots which means that non-encrypted information can be recovered from each of the two time slots by an EXOR operation between the encrypted information.

In accordance with the present invention, the time slot ordinal number or an equivalent to this number is inserted into the frame as a further parameter when encrypting. As a result, when transmitting in two time slots within the same frame, the transmitted information will be independently encrypted and encryption security therewith further enhanced in comparison to the case when only the frame number (in addition to the encryption key) is used. If, as is normal, a user uses only one time slot per frame, no time-slot dependent encryption is required because the user's authorization key is unique for a certain time slot. By modifying the input parameters (code key Kc, frame number FN) in direct dependence on the ordinal number of a time slot in a frame in accordance with the present invention, it is possible to apply the original algorithms without needing to make any substantial change to the signalling protocol, as before described, or to the radio equipment.

Figure 3 is a block diagram illustrating the use of the original algorithm A5 with modified input magnitudes in accordance with the present invention.

The block AB in Figure 3 symbolizes the original algorithm A5, which is specified in accordance with GSM 03.20. The encryption key Kc is now modified in accordance with the ordinal number TSn=TS1 of the relevant time slot, namely the time slot in the frame during which a first block B1 according to Figure 2 shall be transmitted (possibly interfoliated with an adjacent block, although the principle is the same). In this regard, circle 1 symbolizes a calculation algorithm ALG1 for obtaining a modified value Kc1 of the encryption key. The same algorithm can be used for all time slots in the frame, such that

$$ALG1(Kc,TSn) = Kcn'.$$

It is not necessary to modify all encryption keys and one key may be identical to the normal encryption key Kc for a given time slot.

Similarly, the frame ordinal number FN is modified in dependence on the ordinal number TSn=TS1 of the relevant time slot in the frame within which the first block B1 in Figure 2 shall be transmitted. Circle 2 therewith symbolizes a calculation algorithm ALG2 for obtaining the modified value FN' of the frame ordinal number. The same algorithm can be used for all time slots in the frame, such that

$$ALG2(FN,TSn) = FNn'.$$

The two algorithms ALG1 and ALG2 need not be equal.

Furthermore, one of the modified frame numbers FNn' may be identical to the normal FN.

In both of the aforesaid cases, there is obtained an output magnitude in the form of a modified pseudo-random sequence PSm' which is used in the same way as that shown in Figure 2.

It will be understood that the sequence PSm' can also be generated either

a) by solely using a modified value Kc' on the encryption key and an unchanged value FN on the frame number, i.e. the algorithm 2 is not used; or

b) by solely using a modified value FN' on the frame number FN and an unchanged value on the encryption key Kc, i.e. the algorithm 1 is not used.

Figure 4 is a block diagram similar to the block diagram of Figure 3, but now with totally unchanged input values Kc, FN to the algorithm A5. Instead, the time slot ordinal number TSn (or a value equivalent to said ordinal number) is used as a control value for an algorithm ALG3 symbolized by circle 3 for modifying the normal pseudo-random sequence PS obtained from Kc and FN. This algorithm ALG3 may consist in a certain permutation, shift, reordering of values, etc., in the pseudo-random sequence PS, so as to obtain a new sequence PSm'. The sequence may optionally be divided into blocks of 114 bits prior to reformulation, and the values in one or more blocks can be mixed to obtain the new values with an unchanged number of bits (114) in each block.

It is also possible to combine the algorithms ALG1,2 in Figure 3 with the algorithm ALG3 according to Figure 4.

The aforedescribed embodiments of the proposed method relate to transmission cases. It will be understood that in the case of reception wherein incoming information shall be decrypted, the values of Kc and FN and the sequence PS will be modified

to Kc', FN' and PSm' respectively in accordance with the agreed algorithms ALG1, ALG3 and ALG3 as described above.

CLAIMS

1. A method of encrypting information transmitted between a fixed network (MSC, BSS) and a mobile station (MS) in a mobile radio system that operates in accordance with the time division multiple access concept, wherein the information is divided into at least two blocks (B1, B2) and transmitted in at least two time slots (TS1, TS2) corresponding to said blocks in each frame in a frame sequence, and wherein encryption is effected by

a) forming a pseudo-random sequence (PS) in accordance with a given encryption algorithm (A5) from an encryption key (Kc) and the ordinal number (FN) of the frame in which the information is transmitted;

b) performing a logic operation (EXOR) between said pseudo-random sequence (PS) and each block (B1 and B2) of the non-encrypted information to obtain encrypted information (BK1, BK2);

characterized by

c) modifying said encryption key (Kc) in accordance with a given algorithm (ALG1) and in dependence on the ordinal number of a time slot (TSn) so as to obtain a modified encryption key (Kc');

d) forming a modified pseudo-random sequence (PSm') from the resultant modified encryption key (Kc') in accordance with aid encryption algorithm A5); and

e) performing said logic operation (EXOR) on the modified pseudo-random sequence (PSm') and for each block (B1 and B2) of the non-encrypted information.

2. A method according to Claim 1, **characterized** by carrying out the operation performed in accordance with e) on the information block (B1) that belongs to the time slot (TS1) whose ordinal number has been used to form said modified encryption key.

3. A method of encrypting information transmitted between a fixed network (N) and a mobile station (MS) in a mobile radio system that operates in accordance with the time division multiple access concept, wherein the information is divided into at least two blocks (B1, B2) and transmitted in at least two time slots (TS1, TS2) corresponding to said blocks in each frame in a frame sequence, and wherein encryption is effected by

a) forming a pseudo-random sequence (PS) in accordance with a given encryption algorithm (A5) from an encryption key (Kc) and the ordinal number (FN) of the frame in which the information is transmitted;

b) performing a logic operation (EXOR) between said pseudo-random sequence (PS) and each block (B1 and B2) of non-encrypted information to obtain encrypted information (BK1, BK2);

characterized by

c) modifying said frame number (FN) in accordance with a given algorithm (ALG2) and in dependence on the ordinal number of a relevant time slot (TSn);

d) forming a modified pseudo-random sequence (PSm') from the obtained modified frame number (FN') in accordance with said encryption algorithm (A5); and

e) performing said logic operation (EXOR) on the modified pseudo-random sequence (PSm') for each block (B1 and B2) of non-encrypted information.

4. A method of encrypting information transmitted between a fixed network (N) and a mobile station (MS) in a mobile radio system that operates in accordance with the time division multiple access concept, wherein the information is divided into at least two blocks (B1, B2) and transmitted in at least two time slots (TS1, TS2) corresponding to said blocks in each frame in a frame sequence, and wherein encryption is effected by

a) forming a pseudo-random sequence (PS) from an encryption key (Kc) and the ordinal number (FN) of the frame in which

the information is transmitted in accordance with a given encryption algorithm (A5);

b) performing a logic operation (EXOR) between said pseudo-random sequence and each block of the non-encrypted information (INFO1);

characterized by

c) modifying said encryption key (Kc) in accordance with a given algorithm (ALG1) and in dependence on the ordinal number of the relevant time slot (TSn);

d) forming a modified pseudo-random sequence (PSm') from the obtained modified encryption key (Kc') in accordance with said encryption algorithm (A5);

e) modifying said frame number (FN) in accordance with a given algorithm (ALG2) and in dependence on the ordinal number of a relevant time slot (TSn);

f) forming a modified pseudo-random sequence (PSm') from the obtained modified frame number (FN') in accordance with said encryption algorithm (A5); and

g) performing said logic operation (EXOR) on the modified pseudo-random sequence (PSm') for each block (B1 and B2) of the non-encrypted information.

5. A method of encrypting information transmitted between a fixed network (N) and a mobile station (MS) in a mobile radio system that operates in accordance with the time division multiple access concept, wherein the information is divided into at least two blocks (B1, B2) and transmitted in at least two time slots (TS1, TS2) corresponding to said blocks in each frame in a frame sequence, and wherein encryption is effected by

a) forming a pseudo-random sequence (PS) from an encryption key (Kc) and the ordinal number (FN) of the frame in which the information is transmitted in accordance with a given encryption algorithm (A5);

b) performing a logic operation (EXOR) between said pseudo-random sequence and each block of the non-encrypted information (INFO1);

characterized by

c) forming a modified pseudo-random sequence (PSm') from said pseudo-random sequence (PS) in dependence on the ordinal number (TSn) of the time slot within which the information block (B1 or B2) that is encrypted with the modified pseudo-random sequence shall be transmitted in accordance with a given algorithm (ALG3); and

d) performing said logic operation (EXOR) on the modified pseudo-random sequence (PSm') for each block (B1 and B2) of the non-encrypted information.

AMENDED CLAIMS

[received by the International Bureau on 11 February 1997 (11.02.97); original claims 1-5 replaced by new claims 1-5 (3 pages)]

1. A method of encrypting information transmitted between a fixed network (MSC, BSS) and a mobile station (MS) in a mobile radio system that operates in accordance with the time division multiple access concept, wherein the information is divided into at least two blocks (B1, B2) and transmitted in at least two time slots (TS1, TS2) corresponding to said blocks in each frame in a frame sequence, and wherein encryption is effected by

a) forming a pseudo-random sequence (PS) in accordance with a given encryption algorithm (A5) from an encryption key (Kc) and the ordinal number (FN) of the frame in which the information is transmitted;

b) performing a logic operation (EXOR) between said pseudo-random sequence (PS) and each block (B1 and B2) of the non-encrypted information to obtain encrypted information (BK1, BK2);

characterized by

c) modifying said encryption key (Kc) in accordance with a given algorithm (ALG1) and in dependence on the ordinal number of a time slot (TSn) so as to obtain a modified encryption key (Kc');

d) forming a modified pseudo-random sequence (PSm') from the resultant modified encryption key (Kc') obtained from each of the used time slots and in accordance with aid encryption algorithm A5); and

e) performing said logic operation (EXOR) on the modified pseudo-random sequence (PSm') and for the respective block (B1 and B2) of the non-encrypted information.

2. A method according to Claim 1, **characterized** by carrying out the operation performed in accordance with e) on the information block (B1) that belongs to the time slot (TS1) whose ordinal number has been used to form said modified encryption key.

3. A method of encrypting information transmitted between a fixed network (N) and a mobile station (MS) in a mobile radio system that operates in accordance with the time division multiple access concept, wherein the information is divided into at least two blocks (B1, B2) and transmitted in at least two time slots (TS1, TS2) corresponding to said blocks in each frame in a frame sequence, and wherein encryption is effected by

a) forming a pseudo-random sequence (PS) in accordance with a given encryption algorithm (A5) from an encryption key (Kc) and the ordinal number (FN) of the frame in which the information is transmitted;

b) performing a logic operation (EXOR) between said pseudo-random sequence (PS) and each block (B1 and B2) of non-encrypted information to obtain encrypted information (BK1, BK2);

characterized by

c) modifying said frame number (FN) in accordance with a given algorithm (ALG2) and in dependence on the ordinal number of a relevant time slot (TSn);

d) forming a modified pseudo-random sequence (PSm') from the obtained frame number (FN') modified for each of the time slots used and in accordance with said encryption algorithm (A5); and

e) performing said logic operation (EXOR) on the modified pseudo-random sequence (PSm') for the respective block (B1 and B2) of non-encrypted information.

4. A method of encrypting information transmitted between a fixed network (N) and a mobile station (MS) in a mobile radio system that operates in accordance with the time division multiple access concept, wherein the information is divided into at least two blocks (B1, B2) and transmitted in at least two time slots (TS1, TS2) corresponding to said blocks in each frame in a frame sequence, and wherein encryption is effected by

a) forming a pseudo-random sequence (PS) from an encryption key (Kc) and the ordinal number (FN) of the frame in which the information is transmitted in accordance with a given encryption algorithm (A5);

b) performing a logic operation (EXOR) between said pseudo-random sequence and each block of the non-encrypted information (INFO1);

characterized by

c) modifying said encryption key (Kc) in accordance with a given algorithm (ALG1) and in dependence on the ordinal number of the relevant time slot (TSn);

d) forming a modified pseudo-random sequence (PSm') from the obtained encryption key (Kc') modified for each of the time slots used and in accordance with said encryption algorithm (A5);

e) modifying said frame number (FN) in accordance with a given algorithm (ALG2) and in dependence on the ordinal number of a relevant time slot (TSn);

f) forming a modified pseudo-random sequence (PSm') from the obtained modified frame number (FN') in accordance with said encryption algorithm (A5); and

g) performing said logic operation (EXOR) on the modified pseudo-random sequence (PSm') for each block (B1 and B2) of the non-encrypted information.

5. A method of encrypting information transmitted between a fixed network (N) and a mobile station (MS) in a mobile radio system that operates in accordance with the time division multiple access concept, wherein the information is divided into at least two blocks (B1, B2) and transmitted in at least two time slots (TS1, TS2) corresponding to said blocks in each frame in a frame sequence, and wherein encryption is effected by

a) forming a pseudo-random sequence (PS) from an encryption key (Kc) and the ordinal number (FN) of the frame in which the information is transmitted in accordance with a given encryption algorithm (A5);

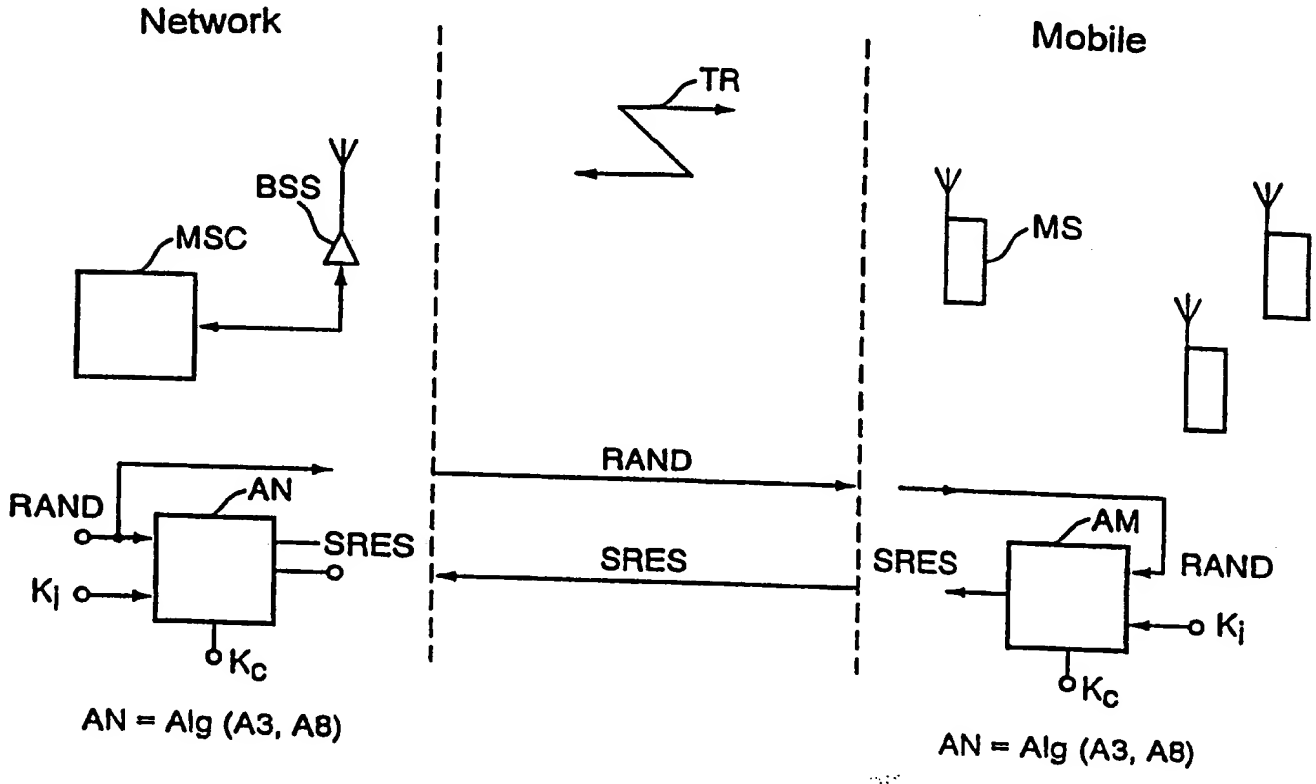

Network
Mobile
TR
BSS
MSC
MS
RAND
AN
SRES
Ki
Kc
RAND
SRES
AM
SRES
RAND
Ki
Kc
AN = Alg (A3, A8)
AN = Alg (A3, A8)

Fig. 1

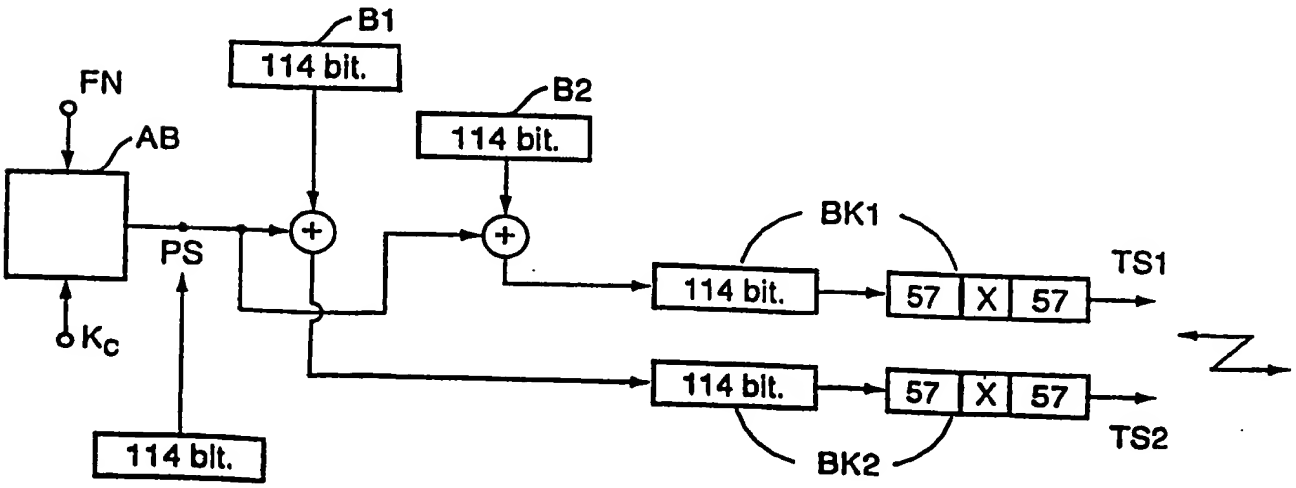

B1
114 bit.
FN
AB
B2
114 bit.
BK1
PS
114 bit.
57
X
57
TS1
Kc
114 bit.
114 bit.
57
X
57
TS2
114 bit.
BK2

Fig. 2

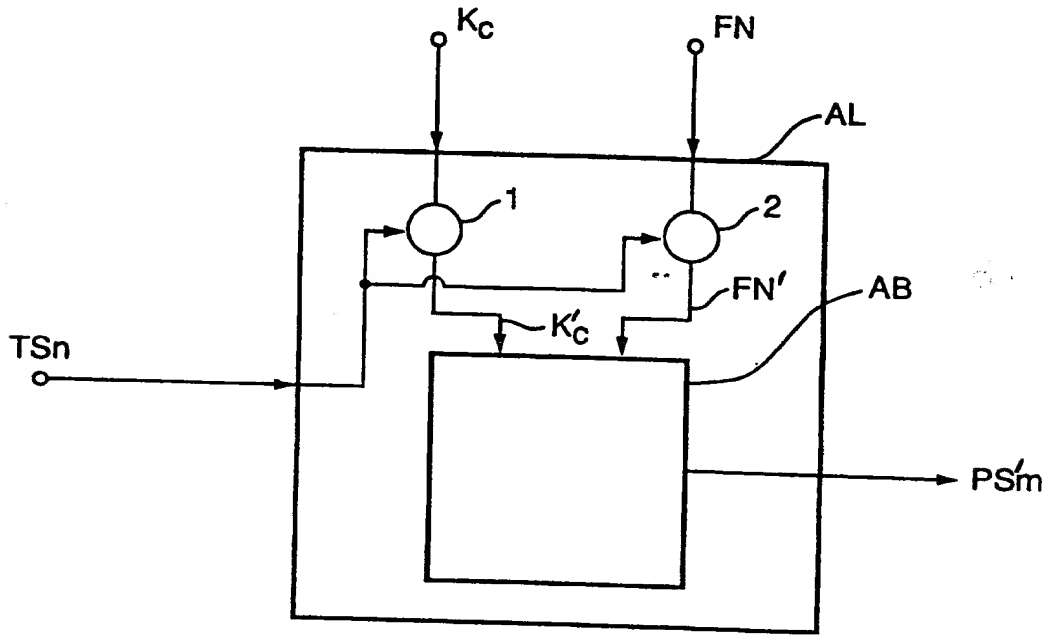


Fig. 3

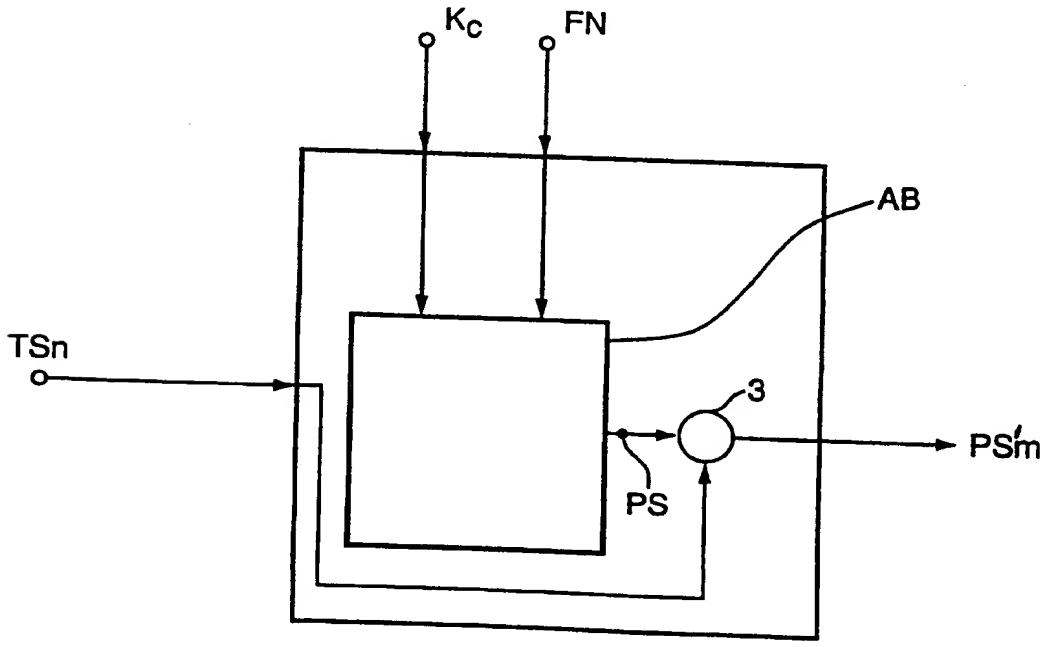


Fig. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 96/01156

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: H04L 9/16, H04Q 7/38
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: H04L, H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5148485 A (PAUL DENT), 15 Sept 1992 (15.09.92), see whole document ---	1-5
A	WO 8800416 A1 (MOTOROLA INC.), 14 January 1988 (14.01.88), see whole document --- --------	1-5

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 January 1997	29 -01- 1997
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Rune Bengtsson Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

Information on patent family members

28/10/96

International application No.
PCT/SE 96/01156

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US-A- 5148485	15/09/92	AU-B- 645464	13/01/94
		AU-A- 8433191	18/02/92
		CA-A- 2087616	21/01/92
		CN-B- 1032039	12/06/96
		CN-A- 1059999	01/04/92
		GB-A,B- 2261348	12/05/93
		HK-A- 29795	10/03/95
		JP-T- 6501350	10/02/94
		KR-B- 9608031	19/06/96
		NZ-A- 238651	27/04/94
		NZ-A- 248445	25/03/94
		SG-A- 178094	12/05/95
		WO-A- 9202089	06/02/92
WO-A1- 8800416	14/01/88	CA-A- 1264355	09/01/90
		DE-A,T- 3786460	12/08/93
		EP-A,B- 0313576	03/05/89
		KR-B- 9600543	08/01/96
		US-A- 4815128	21/03/89